09-06-00

Attorney's Docket No. PNE-203 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): RAM PEMMARAJU

WARNING: *Patent must be applied for in the name(s) of all of the actual inventor(s). 37 CFR 1.41(a) and 1.53(b).*

For (title): OUT-OF-BAND SECURITY NETWORKS FOR COMPUTER NETWORK APPLICATIONS.

CERTIFICATION UNDER 37 CFR 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service on this date 9/1/2000, in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number EK956529164US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

SIEGMAR SILBER
(type or print name of person mailing paper)

Siegmar Silber
Signature of person mailing paper

NOTE: Each paper or fee referred to as enclosed herein has the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 CFR 1.10(b).

WARNING: *Certificate of mailing (first class) or facsimile transmission procedures of 37 CFR 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.*

1. Type of Application

This new application is for a(n)

(check one applicable item below)

☒ Original (nonprovisional)

□ Design

□ Plant

WARNING: ***Do not*** *use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application.*

WARNING: ***Do not*** *use this transmittal for the filing of a provisional application.*

NOTE: *If one of the following 3 items apply, then complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED and a NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION.*

□ Divisional.

□ Continuation.

□ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. 119(e), 120, or 121)

NOTE: *If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.*

WARNING: *If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. 120, 121 or 365(c), the 20–year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. 120, 121 or 365(c). (35 U.S.C. 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. 119, 365(a) or 365(b).) For a c–i–p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.*

WARNING: *When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application* ***must*** *be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).*

□ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed That Are Required for Filing Date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

26 Pages of specification

7 Pages of claims

1 Pages of Abstract

14 Sheets of drawing

☒ formal

□ informal

WARNING: ***DO NOT*** *submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. Comments on proposed new 37 CFR 1.84. Notice of March 9, 1988 (1990 O.G. 57-62).*

NOTE: "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm. (5/8 inch) down from the top of the page." 37 C.F.R. 1.84(c)).

(complete the following, if applicable)

□ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. 1.84(b).

4. Additional papers enclosed

□ Preliminary Amendment

□ Information Disclosure Statement (37 C.F.R. 1.98)

□ Form PTO-1449 (PTO/SB/08A and 08B)

□ Citations

□ Declaration of Biological Deposit

□ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.

□ Authorization of Attorney(s) to Accept and Follow Instructions from Representative

□ Special Comments

□ Other

5. Declaration or oath

☒ Enclosed

Executed by

(check **all** *applicable boxes)*

☒ inventor(s).

□ legal representative of inventor(s).
37 CFR 1.42 or 1.43.

□ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.

□ This is the petition required by 37 CFR 1.47 and the statement required by 37 CFR 1.47 is also attached. *See* item 13 below for fee.

□ Not Enclosed.

WARNING: *Where the filing is a completion in the U.S. of an International Application, but where a declaration is not available, or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.*

□ Application is made by a person authorized under 37 C.F.R. 1.41(c) on behalf of *all* the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 CFR 1.16(e) can be filed subsequently).

NOTE: *It is important that all the correct inventor(s) are named for filing under 37 CFR 1.41(c) and 1.53(b).*

□ Showing that the filing is authorized.
(not required unless called into question. 37 CFR 1.41(d))

6. Inventorship Statement

WARNING: *If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.*

The inventorship for all the claims in this application are:

☒ The same.

or

□ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

□ is submitted.

□ will be submitted.

7. Language

NOTE: *An application including a signed oath or declaration may be filed in a language other than English. A verified English translation of the non-English language application and the processing fee of $130.00 required by 37 CFR 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 CFR 1.52(d).*

NOTE: *A non-English oath or declaration in the form provided or approved by the PTO need not be translated. 37 CFR 1.69(b).*

☒ English

□ Non-English

□ The attached translation is a verified translation. 37 C.F.R. 1.52(d).

8. Assignment

☒ An assignment of the invention to NET SECURE, L. L. C.

☒ is attached. A separate ☒ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or □ FORM PTO 1595 is also attached.

□ will follow.

NOTE: *"If an assignment is submitted with a new application, send two separate letters-one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).*

WARNING: *A newly executed "CERTIFICATE UNDER 37 CFR 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.*

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. no.	Filed
Country	Appln. no.	Filed
Country	Appln. no.	Filed

from which priority is claimed

□ is (are) attached.

□ will follow.

NOTE: *The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 CFR 1.55(a) and 1.63.*

NOTE: *This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.*

10. Fee Calculation (37 C.F.R. 1.16)

A. ☑ Regular application

CLAIMS AS FILED

Number filed	Number Extra		Rate	Basic Fee 37 C.F.R. 1.16(a) $690.00
Total Claims (37 CFR 1.16(c)) 12– 20 =		×	$ 22.00	–0–
Independent Claims (37 CFR 1.16(b)) 2– 3 =		×	$ 80.00	–0–
Multiple dependent claim(s), if any (37 CFR 1.16(d))	0	+	$260.00	–0–

□ Amendment cancelling extra claims is enclosed.

□ Amendment deleting multiple-dependencies is enclosed.

□ Fee for extra claims is not being paid at this time.

NOTE: *If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 CFR 1.16(d).*

Filing Fee Calculation $ 690.–

B. □ Design application
($320.00—37 CFR 1.16(f))

Filing Fee Calculation $__________

C. □ Plant application
($530.00—37 CFR 1.16(g))

Filing fee calculation $__________

11. Small Entity Statement(s)

☒ Verified Statement(s) that this is a filing by a small entity under 37 CFR 1.9 and 1.27 is (are) attached.

WARNING: *"Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. A nonprovisional application claiming benefit under 35 U.S.C. 119(e), 120, 121 or 365(c) of a prior application may rely on a verified statement filed in the prior application if the nonprovisional application includes a reference to a verified statement in the prior application or includes a copy of the verified statement filed in the prior application if status as a small entity is still proper and desired." 37 C.F.R. § 1.28(a).*

(complete the following, if applicable)

□ Status as a small entity was claimed in prior application _____ / __________, filed on __________, from which benefit is being claimed for this application under:

35 U.S.C. □ 119(e),
□ 120,
□ 121,
□ 365(c),

and which status as a small entity is still proper and desired.

□ A copy of the verified statement in the prior application is included.

Filing Fee Calculation (50% of **A, B** or **C** above)

$ 345. –

NOTE: Any excess of the full fee paid will be refunded if a verified statement and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 CFR 1.28(a).

12. Request for International-Type Search (37 C.F.R. 1.104(d))

(complete, if applicable)

□ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

□ Not Enclosed

□ No filing fee is to be paid at this time.
(This and the surcharge required by 37 C.F.R. 1.16(e) can be paid subsequently.)

☒ Enclosed

☒ Basic filing fee $ 345. –

☒ Recording assignment
($40.00; 37 C.F.R. 1.21(h))
(See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION".) $ 40. –

□ Petition fee for filing by other than all the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached
($130.00; 37 C.F.R. 1.47 and 1.17(h)) $ ____________

□ For processing an application with a specification in a non-English language
($130.00; 37 C.F.R. 1.52(d) and 1.17(k)) $ ____________

□ Processing and retention fee
($130.00; 37 C.F.R. 1.53(d) and 1.21(l)) $ ____________

□ Fee for international-type search report
($40.00; 37 C.F.R. 1.21(e)) $ ____________

NOTE: *37 CFR 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 CFR 1.53(d) and this, as well as the changes to 37 CFR 1.53 and 1.78, indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from notification under § 53(d).*

Total fees enclosed $ 385. –

14. Method of Payment of Fees

☒ Check in the amount of $ 385. –

□ Charge Account No. ____________ in the amount of $____________.

A duplicate of this transmittal is attached.

NOTE: *Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 CFR 1.22(b).*

15. Authorization to Charge Additional Fees

WARNING: *If no fees are to be paid on filing, the following items should not be completed.*

WARNING: *Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.*

□ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. ____________:

□ 37 C.F.R. 1.16(a), (f) or (g) (filing fees)

□ 37 C.F.P. 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: *Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 CFR 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.*

□ 37 C.F.R. 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

□ 37 C.F.R. 1.17 (application processing fees)

WARNING: *While 37 CFR 1.17(a), (b), (c) and (d) deal with extensions of time under § 1.136(a), this authorization should be made only with the knowledge that: "Submission of the appropriate extension fee under 37 C.F.R. 1.136(a) is to no avail unless a request or petition for extension is filed." (Emphasis added). Notice of November 5, 1985 (1060 O.G. 27).*

□ 37 C.F.R. 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. 1.311(b))

NOTE: *Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 CFR 1.311(b).*

NOTE: *37 CFR 1.28(b) requires "Notification of any change in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . issue fee." From the wording of 37 CFR 1.28(b): (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.*

16. Instructions as to Overpayment

□ Credit Account No. ____________

□ Refund

Siegmar Silber
SIGNATURE OF ATTORNEY

Reg. No. 26,233

SIEGMAR SILBER
(type or print name of attorney)

Tel. No. (973) 779 2580

66 MOUNT PROSPECT AVE.
P.O. Address
CLIFTON, NEW JERSEY 07013

☐ **Incorporation by reference of added pages**

(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)

☐ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added ______________

☐ Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added ______________

☐ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added ______________

☒ **Statement Where No Further Pages Added**

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

☒ This transmittal ends with this page.

ADDED PAGE(S) FOR SPECIAL COMMENTS FOR NEW APPLICATION TRANSMITTAL

Added page______________________________________

ATTORNEY'S DOCKET NO. PNE-203 **PATENT**

□ Applicant □ Patentee________________

□ Application No. □ Patent No.________________

□ Filed on □ Issued on________________

Title: OUT-OF-BAND SECURITY NETWORKS FOR COMPUTER APPLICATION

VERIFIED STATEMENT CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) and 1.27(c)-SMALL BUSINESS CONCERN

I hereby declare that I am

□ the owner of the small business identified below

☒an official of the small business concern empowered to act on behalf of the concern identified below:

Name of Small Business Concern NET SECURE L.L.C.

Address of Small Business Concern 81 MARY STREET
LODI, NJ 07644

I hereby declare that the above-identified small business qualifies as a small business concern, as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office under Sections 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control both.

I hereby declare that the rights under contract or law have been conveyed to, and remain with, the small business concern identtified above, with regard to the invention described in

□ the specification filed herewith, with title as listed above.

□ the application identified above.

□ the patent identified above.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern, or organizationhaving rights in the invention is listed below and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c), if that person had made the invention, or to any concern that would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

NOTE: Separate verified statements are required from each named person, concern, or organization having rights to the invention averring to their status as small entities (37CFR1.27).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

□ No such person, concern, or organization exists.

□ Each such person, concern or organization is listed below.*

*NOTE: Separate verified statements are required from each named person, concern organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

FULL NAME: ROBERT J. KOCH

ADDRESS : 81 MARY STREET, LODI, NEW JERSEY 07644

□ INDIVIDUAL □ SMALL BUSINESS CONCERN □ NONPROFIT ORGANIZATION

FULL NAME

ADDRESS

□ INDIVIDUAL □ SMALL BUSINESS CONCERN □ NONPROFIT ORGANIZATION

FULL NAME

ADDRESS

□ INDIVIDUAL □ SMALL BUSINESS CONCERN □ NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on high status as a small entity is not longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Name of Person Signing ROBERT J. KOCH

Title of Person if Other Than Owner VICE PRESIDENT

Address of Person Signing 81 MARY STREET

LODI, NEW JERSEY 07644

SIGNATURE DATE 09/01/2000

patapps/abocatch.smb

TITLE: OUT-OF-BAND SECURITY NETWORKS FOR COMPUTER NETWORK APPLICATIONS

BACKGROUND OF THE INVENTION

1. Field of the Invention.

This invention relates to security networks for computer network applications, and, more particularly, to a security network which provides user authentication by an out-of-band system that is entirely outside the host computer network being accessed. In addition, the out-of-band system optionally includes provision for biometric identification as part of the authentication process.

2. Background of the Invention.

In the past, there have typically been three categories of computer security systems, namely, access control, encryption and message authentication, and intrusion detection. The access control systems act as the first line of defense against unwanted intrusions, and serve to prevent hackers who do not have the requisite information, e.g. the password, etc., from accessing the computer networks and systems. Secondly, the encryption and message authentication systems ensure that any information that is stored or in transit is not readable and cannot be modified. In the event that a hacker is able to break into the computer network, these systems prevent the information from being understood, and, as such, encryption systems act as the second line of defense. Further, intrusion detection systems uncover patterns of hacker attacks and viruses and, when discovered provide an alarm to the system administrator so that appropriate action can be taken. Since detection systems operate only after a hacker has successfully penetrated a system, such systems act as a third line of defense.

Obviously, as an access control system is the first line of defense, it is important that the selection thereof be well-suited to the application. In access control systems there is a broad dichotomy between user authentication and host authentication systems. In current practice, the most common user authentication systems include simple password systems, random password systems, and biometric systems. The simple password systems are ubiquitous in our society with every credit card transaction using a pin identification number, every automatic teller machine inquiry looking toward a password for access, and even telephone answering messages using simple password systems for control. To this in random password systems another level of sophistication is added. In these systems, the password changes randomly every time a system is accessed. These systems are based on encryption or a password that changes randomly in a manner that is synchronized with an authorization server. The Secure ID card is an example of such a system. Random password systems require complimentary software and/or hardware at each computer authorized to use the network. In biometric systems, characteristics of the human body (such as voice, fingerprints or retinal scan) are used to control access. These systems also require software and/or hardware at each computer which is authorized to use the network. The other category of access control is that of host authentication. Here the commonest systems are those of "call back" and "firewall" systems. Call back systems are those systems which work by calling a computer back at a predetermined telephone number. These systems authenticate the location of a computer and are suitable for dial-up (modem) networks; however, such systems are ineffective when the attack comes via the Internet. On the other hand, firewall systems are designed to prevent attacks coming from the Internet and work by allowing access only from computers within a network. Even though firewall systems are implemented either as standalone systems or incorporated into routers, a skilled hacker is still able to bypass such a host authentication system.

Currently, all the security products that perform access control are based on "in-band" authentication - i.e. the data and authentication information are on the same network. For example, upon accessing a computer, a computer prompt requests that you enter your password (authentication information) and, upon clearance, access is granted. In this example, all information exchanged is on the same network or may be termed "in-band." The technical problem which arises is that the hacker is then placed in a self-authenticating environment.

Except for callback systems, typically the access control products authenticate only the user and not the location. At a time when computer networks could only be accessed by modems, the authentication of location by dialing back the computer which requested the access provided a modicum of security. Now as virtually all the computer networks are accessible by the Internet, which is modem independent, location authentication by callback is not secure. The lack of security arises as there is no necessary connection between the Internet address and a location, and, in fact, an Internet address most often changes from connection to connection. Thus, callback systems are rendered useless against attacks originating from the Internet.

In preparing for this application, a review of various patent resources was conducted. The review resulted in the inventor gaining familiarity with the following patents:

ITEM NO.	PAT. NO.	INVENTOR	ORIG. CLASS	ISSUE DATE
1	5,898,830	Wesinger ***et al.***	395/187.01	04/27/1999
2	5,680,458	Spelman ***et al.***	380/21	10/21/1997
3	5,615,277	Hoffman	382/115	03/25/1997
4	5,588,060	Aziz	380/30	12/24/1996
5	5,548,646	Aziz ***et al.***	380/23	08/20/1996

In general terms, the patents all show a portion of the authentication protocol conducted out-of-band. For purposes of this discussion an "out-of-band" operation is defined as one conducted without reference to the host computer or any database in the host network.

In Item 1, the patent to Wesinger ***et al.***, U.S. Patent

5,898,830 (‘830) is a firewall patent. Here, the inventor attempts to enhance security by using out-of-band authentication. In his approach, a communication channel, or medium, other than the one over which the network communication takes place, is used to transmit or convey an access key. The key is transmitted from a remote location (e.g, using a pager or other transmission device) or and, using a hardware token, the key is to the conveyed local device. In the ‘830 system, to gain access, a hacker must have access to a device (e.g., a pager, a token etc.) used to receive the out-of-band information. Pager beep-back or similar authentication techniques may be especially advantageous in that, if a hacker attempts unauthorized access to a machine while the authorized user is in possession of the device, the user will be alerted by the device unexpectedly receiving the access key. The key is unique to each transmission, such that even if a hacker is able to obtain it, it cannot be used at other times or places or with respect to any other connection.

Next turning to Item 2, the patent to Spelman ***et al.***, U.S. Patent 5,680,458 (‘458), a method of recovering from the compromise of a root key is shown. Here, following the distribution of a new replacement key, an out-of-band channel is used by a central authority to publish a verification code which can be used by customers to verify the authenticity of the emergency message. The ‘458 patent further indicates that the central authority uses the root key to generate a digital signature which is appended to the emergency message to verify that the emergency message is legitimate.

Hoffman, U.S. Patent 5,615,277, is next discussed. Here, biometrics are combined with a tokenless security and the patent describes a method for preventing unauthorized access to one or more secured computer systems. The security system and method are principally based on a comparison of a unique biometric sample, such as a voice recording, which is gathered directly from the person of an unknown user with an authenticated unique biometric sample of the same type. The Hoffman technology is networked to act as a full or partial intermediary between a secured computer system and its authorized users. The security system and method further contemplate the use of personal codes to confirm identifications determined from biometric comparisons, and the use of one or more variants in the personal identification code for alerting authorities in the event of coerced access.

Items 4 and 5 have a common assignee, Sun Microsystems, Inc., and both concern encryption/decryption keys and key management.

The submission of the above list of documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. None of the above show the novel and unobvious features of the invention described hereinbelow.

SUMMARY

In general terms, the invention disclosed hereby includes in the embodiments thereof, a unique combination of user and host authentication. The security system of the present invention is out-of-band with respect to the host computer and is configured to intercept requests for access. The first step in controlling the incoming access flow is a user authentication provided in response to prompts for a user identification and password. After verification at the security system, the system operating in an out-of-band mode, uses telephone dialup for location authentication and user authentication via a password entered using a telephone keypad. In addition and optionally the system provides further authentication using a biometric system. When voice recognition is employed for the biometric component, the user speaks a given phrase which the system authenticates before permitting access. Upon granting of access, the user now for the first time enters the in-band operating field of the host computer.

OBJECT AND FEATURES OF THE INVENTION

It is an object of the present invention to provide a host computer with a cost effective, out-of-band security network that combines high security and tokenless operation.

It is a further object of the present invention to provide a network to isolate the authentication protocol of a computer system from the access channel therefor.

It is yet another object of the present invention to provide a separate security network which acts conjunctively with or as an overlying sentry box to the existing security system provided by the host computer.

It is still yet another object of the present invention to provide an authentication using a biometric component, such as speech recognition, to limit access to specific individuals.

It is a feature of the present invention that the security network achieves high security without encryption and decryption.

It is another feature of the present invention to have a callback step that restricts authentication to a given instrument thereby enabling restriction to a fixed location.

It is yet another feature of the present invention to combine callback and speech recognition in an out-of-band security facility.

Other objects and features of the invention will become apparent upon review of the drawings and the detailed description which follow.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following drawings, the same parts in the various views are afforded the same reference designators.

FIG. 1 is a schematic diagram of the security system of the present invention as applied to the internet in which an external accessor in a wide area network seeks entry into a host system;

FIG. 2 is a schematic diagram of the apparatus required for the security system shown in FIG. 1;

FIG. 3 is a schematic diagram of the software program required for the security system shown in FIG. 1 in which various program modules are shown for corresponding functions of the system and each module is shown in relation to the control module thereof;

FIG. 4 is a detailed schematic diagram of the software program required for the line module of the security system shown in FIG. 3;

FIG. 5 is a detailed schematic diagram of the software program required for the speech module of the security system shown in FIG. 3;

FIG. 6 is a detailed schematic diagram of the software program required for the administration module of the security system shown in FIG. 3;

FIG. 7 is a detailed schematic diagram of the software program required for the client/server module of the security system shown in FIG. 3;

FIG. 8 is a detailed schematic diagram of the software program required for the database module of the security system shown in FIG. 3;

FIG. 9A through 9E is a flow diagram of the software program required for the security system shown in FIG. 1; and,

FIG. 10 is a schematic diagram of a second embodiment of the security system of the present invention as applied to the intranet in which an internal accessor in a local area network seeks entry into a restricted portion of the host system.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The out-of-band security system networks for computer network applications is described in two embodiments. The first describes an application to a wide area network, such as the internet, wherein the person desiring access and the equipment used thereby are remote from the host computer. The second embodiment describes the application of the disclosed invention to a local area network wherein the person desiring access and the equipment used thereby are within the same network (referred to as the "corporate network") as the host computer. For purposes of this description the person desiring access and the equipment used thereby are referred collectively as the "accessor".

In Figure 1, a general overview of the first embodiment of the out-of-band security networks for computer network applications of this invention is shown and is referred to generally by the reference designator 20. Here the accessor is the computer equipment 22, including the central processing unit and the operating system thereof, and the person or user 24 whose voice is transmittable by the telephone 26 over telephone lines 28. The access network 30 is constructed in such a manner that, when user 24 requests access to a web page 32 located at a host computer or web server 34 through computer 22, the request-for-access is diverted by a router 36 internal to the corporate network 38 to an out-of-band security network 40. Authentication occurs in the out-of-band security network 40, which is described in detail below. This is in contradistinction to present authentication processes as the out-of-band security network 40 is isolated from the corporate network 38 and does not depend thereon for validating data. The first shows a biometric validation which, in this case, is in the form of voice recognition and is within voice network 42. While voice recognition is used herein, it is merely exemplary of many forms of recognizing or identifying an individual person. Others include, but are not limited to fingerprint identification, iris recognition; retina identification, palms recognition, and face recognition. Each of these are similar to the first embodiment in that these is a requirement for monitoring the particular parameter of the individual person; including the parameter to a mathematical representation or algorithm therefore; retrieving a previously stored sample (biometric data), thereof from a database and comparing the stored sample with the input of the accessor.

Referring now to Figure 2 a block diagram is shown for the hardware required by the out-of-band security network for computer network applications of this invention. The request-for-access is forwarded from the router 36 of the corporate network to a data network interface 50 which, in turn, is constructed to transfer the request to a dedicated, security network computer 52 over a data bus 48. The computer 52 is adapted to include software programs, see ***infra,*** for receiving the user identification and for validating the corresponding password, and is further adapted to obtain the user telephone number from lookup tables within database 54 through data bus 48. The computer 52 is equipped to telephone the user through a PBX interface 56 and voice bus 58. For voice recognition, a speech or biometric system 60 is provided to process requested speech phrases repeated by the user 24 which is verified within the security computer 52. Upon authentication, access is granted through the data network interface 50.

Referring now to Figures 3 through 8 the software architecture supporting the above functions is next described. The security computer 52, Figure 2, is structured to include various functional software modules, Figure 3, namely, a control module 62, a line module 64, a speech module including a biometric for voice recognition 66, an administration module 68, a client/server module 70, and a database module 72. The software program of the control module 62 functions and interconnects with the other modules (line, speech, administration, client/server and database modules) to control the processing flow and the interfacing with the internal and external system components. As will be understood from the flow diagram description, ***infra***, the control module 62 software of the security computer 52 incorporates a finite state machine, a call state model, process monitors, and fail-over mechanisms. The software program of the line module 64 is structured to provide an interface with the telephone network. The software program of the speech module 66 is structured to perform processing functions such as, but not limited to, speech verification, text-to-speech conversion and announcements. The software program of the administration module 68 is structured to archive the records of each call made, to provide security and management functions, and to process any alarms generated. The software program of the client/server module 70 is structured to enable a host computer or a web server 34 to interface with the out-of-band security network 40. The software program of the database module 72 is comprised of the databases to support the security network 40 which in the present invention includes an audit database, a subscriber database, a speech database, an announcement database, and a system database.

Referring now to Figure 4, the line module 64 is described in further detail. The analog telephone interface 74 is the equipment, such as voice bus 58 and PBX interface 56, that interfaces to an analog line. The analog telephone interface 74 is, in turn, controlled by software program of the analog line driver 76. Similarly, digital telephone interface 78 is the equipment, such as data bus 48 and PBX interface 56, that interfaces to a digital line (T1 or ISDN PRI). The digital telephone interface 78 is, in turn, controlled by the software program of the digital line driver 80. The software program of the telephony functions module 82 is structured to accommodate functions such as, ***Call Origination, Call Answer, Supervisory*** signaling, ***Call Progress*** signaling, ***Ring*** generation/detection, ***DTMF*** generation/detection, and line configuration.

In Figure 5 the speech module 66 architecture is detailed. The speech verification (SV) hardware 84, (part of speech system 60, Figure 2) consists of digital signal processors that utilize SV algorithms for verification of an accessor's spoken password. The speech verification hardware 84 is controlled by the software program of the SV hardware driver 86. The software program of the speech verification processing unit 88 provides an interface with control module 62 and is structured to respond to queries therefrom for verifying an accessor's spoken password. Also, the SV processing unit 88 enables the enrollment of users with the speech password and the interaction of the speech database of database module 72. The text-to-speech (TTS) hardware 90 consists of digital signal processors that utilize TTS algorithms. The text-to-speech hardware 90 is controlled by the software program of the TTS hardware driver 92. The software program of the TTS processing unit 94 provides an interface with the control module 62 and, as required by the control module 62, converts text strings to synthesized speech. The announcement hardware 96 consists of digital signal processors that utilize speech algorithms to record and play announcements. The announcement hardware is controlled by the software program of the announcement hardware driver 98. The software program of the announcement processing unit 100 also provides an interface with control module 62; upon demands of the control module 62, supplies stored announcements; and interacts with the announcement database of database module 72.

In Figure 6, the software program of the administration module 68 is presented in more detail. As the administration module 68 interfaces with the control module 62, see ***supra***, a subprogram, namely, a control module interface 102 is constructed to manage the communication therebetween. The administration module 68 further includes software to provide an audit trail of all calls requesting access. This unit or audit log 104 creates records about each call, which records are stored in the audit database of the database module 72. Any alarms caused as a result of errors, threshold crossing or system failures are processed by the software program of alarm module 106. For remote administration of the out-of-band security system 40 of this invention, the software program of the network interface 108 is provided, which software communicates with the corporate network 38 (via network adapters). Access to the out-of-band security system 40 for administrative purposes is controlled by security module 110. Similar to the network interface 108, the software program of the management module 112 provides for the remote management of the out-of-band security system 40 for configuration, status reporting, software upgrades and trouble-shooting purposes.

Referring now to Figure 7, the software program of the client/server module 70 that secures the host computer or web server or router 34 of the corporate network 38 through the out-of band security system 40 of this invention is shown in detail. Here, the client protocol module 114 provides the interfacing means for the host computer or web server 34 and communicates with the out-of band security system 40 using a proprietary protocol. Alternatively, standard protocols such as RADIUS and TACACS can be used. The server protocol module 116 interfaces with the control module 62 and manages the interaction with the client protocol module 114.

In Figure 8 a detailed schematic diagram is shown of the software program required for the database module 72 of the out-of-band security system 40 of this invention. The database module 72 is the recordkeeping center, the lookup table repository, and the archival storehouse of the system. In the above description numerous relationships to this module have already been drawn. The database module 72 communicates through control module interface 118 to the control module 62. Two types of communications are channeled to and from the database module 72, namely, communicating data for use during operations through database access interface 120 and communicating data for maintenance and provisioning of the out-of-band security system through database provisioning interface 122. While the databases described herein are specifically related to the application of this embodiment to voice recognition the formation of specific databases, e.g. a different set of samples of biometric parameters or characteristics, is within the contemplation of the invention. The databases hereof are the audit database 124 for the call records; the subscriber database 126 for subscriber information; the speech database 128 for aid in verifying an accessor's spoken password; the announcements database 130 for announcements to be played to users during a call; and, system database 132 for system related information (e.g. configuration parameters).

In Figure 9A through 9E the flow diagram for the above software program operation is shown and is described hereinbelow. Thus, while the preceding in discussing the network architecture for the out-of-band security system 40 explains the access portion of the program - the operations side - and the configuration and maintenance portion of the program - the provisioning side, the description which follows is of the software operation of the out-of-band security system 40 from the receipt of a request-to-access inquiry to a granting-of-access or denial-of-access result. The logic description that follows reflects the accessor's inputs and the programmed processes along the logical pathway from the receipt of a request-to-access inquiry to a granting-of-access or denial-of-access result. The pathway commences at the **REQUEST FOR ACCESS** block 150 whereby a request to enter the host computer or web server 34 is received from the user at the remote computer 22. The user requesting access to the host computer from the remote computer is immediately prompted to login at the **LOGIN SCREEN PRESENTED** block 152. While the login procedure here comprises the entry of the user identification and password and is requested by the host computer 34, such information request is optionally a function of the security computer 40. Upon entry of data by user at the **ENTRY OF ID AND PASSWORD** block 154 the information is passed to the security computer 40. As described in the software architecture review, ***supra***, the software pathway of the login data is first to client module 114 at **SEND LOGIN DATA TO CLIENT MODULE** block 156 and then successively to server module 116 at **SEND LOGIN DATA TO SERVER MODULE** block 158 and to control module 62 at **SEND LOGIN DATA TO CONTROL MODULE** block 160. In transmitting the login data from the client module 114 to the server module a proprietary protocol is employed, which protocol includes encryption of the data using standard techniques. The verification process is continued at the control module 62 which next enters the subscriber database 126 and retrieves at **CONTROL MODULE QUERIES SUBSCRIBER DATABASE AND RETRIEVES PASSWORD ASSOCIATED WITH LOGIN ID** block 162 the password associated with the logged in identification. The control module 62 verifies at **CONTROL MODULE VERIFIES PASSWORD** block 164 that the password received from the remote computer 22 is the same as the password retrieved from the subscriber database 126. Upon verification, the control module 62 at **DOES THE PASSWORD MATCH?** block 166 sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the control module 62 at **DOES THE PASSWORD MATCH?** block 166 initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. Alternatively, the program offers the user an opportunity to retry whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. The retry process may be limited to a specified number of times. The message that the verification has been achieved is transmitted along the software pathway substantially in the reverse manner as the login data transmission. From the control module 62, the verification is first received by the server module 116 and at **SEND VERIFICATION FROM SERVER MODULE TO CLIENT MODULE** block 168 the verification message along with the information that the authentication is proceeding is transmitted to the client module 114. In transmitting these messages to the client module 114 from the server module a proprietary protocol is employed, which protocol includes decryption of the data, where required, using standard techniques. The client module 114 transmits at **SEND VERIFICATION FROM CLIENT MODULE TO HOST COMPUTER** block 170 the messages to the host computer 34. Finally, the host computer 34 transmits at **SEND VERIFICATION FROM HOST COMPUTER TO REMOTE COMPUTER** block 172 the message that the login verification is complete is sent to the remote computer 22 and prompts the person or user 24 to stand by for a telephonic callback.

Now with the control module 62 having verified the remote computer 22, the software program hereof is constructed to have the control module 62 at **CALLBACK INITIATED BY CONTROL MODULE** block 174 initiate out-of-band the call-back procedure to the user 24. The control module 62 queries the subscriber database 126 and retrieves therefrom the telephone number associated with the login identification. Based on the data retrieved from the subscriber database, the control module 62 instructs the line module 64 at **DIAL USER TELEPHONE NUMBER** block 176 to call user 24. Upon user 24 answering the telephone at **USER ANSWERS TELEPHONE** block 178, the software pathway continues with the line module 64 relaying to the control module 62 at **CONTROL MODULE NOTIFIED BY LINE MODULE OF OFF-HOOK CONDITION** block 180 that the user's telephone is off-hook. The program is constructed so that the control module 62 then instructs the speech module 66 at **SPEECH MODULE INSTRUCTED BY CONTROL MODULE TO RETRIEVE PASSWORD** block 182 to retrieve (or generate) a DTMF password. To accomplish this, the speech module 66 now queries the announcement database 130 and at **PROMPT RETRIEVED BY SPEECH MODULE** block 184 retrieves the prompt to be played to the user 24. Alternatively, the password for the prompt is generated and synthesized by the text-to-speech system 90, 92 and 94 of the speech module 66. At **PROMPT PLAYED BY SPEECH MODULE TO USER** block 186, the user 24 is instructed to impress the DTMF password on the telephone keypad. The program progresses so that after the user 24 enters the DTMF password on the telephone keypad at **USER ENTERS DTMF PASSWORD** block 188, the line module 64 at **LINE MODULE TRANSMITS ENTRY TO CONTROL MODULE** block 190 notifies the control module 62 of the entry made by user 24. In a manner similar to the login password, ***supra,*** the control module 62 queries the subscriber database and, at **CONTROL MODULE RETRIEVES DTMF PASSWORD** block 192, retrieves the password or the generated password associated with the subscriber. At **CONTROL MODULE VERIFIES DTMF PASSWORD** block 194, the control module 62 verifies that the password entered at the telephone keypad by the user matches the password retrieved from the subscriber database. Upon verification, the control module 62 at **DOES THE DTMF PASSWORD MATCH?** block 196 sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the control module 62 at **DOES THE DTMF PASSWORD MATCH?** block 196 initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. As in the previous password verification and alternatively, the program offers the user an opportunity to retry. Whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. As before, the retry process may be limited to a specified number of times.

Upon out-of-band callback verification being received, the biometric identification portion of the software program is initiated. In this present embodiment, while the biometric parameter that is monitored is speech, any of a number of parameters may be used. In this case, the control module 62 instructs the speech module 66 at **SPEECH MODULE RETRIEVES PROMPT FOR USER** block 198 to retrieve a prompt that for the purpose of later playing the prompt to the user and collecting the speech password. The speech module 66 queries the announcement database 130 and retrieves the prompt to be played to the user 24. Besides using a prepared prompt, as above, a prompt synthesized by the text-to-speech system 90, 92 and 94 is utilizable for this purpose.

The prompt for collecting the speech password is played to the user 24 at **PROMPT USER AND COLLECT SPEECH PASSWORD** block 200. The user 24, who has previously had his biometric sample namely the speech pattern, registered with the speech database 128, then voices the speech password at **USER VOICES SPEECH PASSWORD** block 202 and transmits the same over the telephone at the remote computer 22 to the security computer 40. Then, at **SPEECH MODULE RETRIEVES SPEECH PASSWORD ASSOCIATED WITH LOGIN ID** block 204, the software program for the speech module 66 is adapted to query the speech database 128 and to retrieve the speech password associated with the accessor's login identification. Through the application of biometric analysis, such as voice recognition technology, the speech or module 66 at **SPEECH MODULE VERIFIES SPEECH PASSWORD** block 206 verifies that the voiced speech password received from the user 24 has the same pattern as the speech password retrieved from database 128. Upon verification, the speech module 66 at **DOES THE SPEECH PASSWORD MATCH?** block 208 sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the speech module 66 at **DOES THE SPEECH PASSWORD MATCH?** block 208 notifies the control module 62 which initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. As in the previous password verification and alternatively, the program offers the user an opportunity to retry. Whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. As before, the retry process may be limited to a specified number of times. Upon being notified of a match between the pattern of the voiced speech password and that of the one retrieved from the database 128, the control module 62 at **CONTROL MODULE INSTRUCTS SPEECH MODULE TO ANNOUNCE ACCESS IS GRANTED** block 210 instructs the speech module 66 to provide an announcement to the user 24 indicating that access is granted. The speech module 66 queries the announcement database 130 and retrieves the announcement for the user 24. Alternatively, the announcement can be synthesized by the text-to-speech system 90, 92 and 94 and played to the user 24. Whichever announcement is used, it is made to the user at **ACCESS GRANTED ANNOUNCEMENT MADE TO USER** block 212.

Upon completion of the announcement at **SPEECH MODULE NOTIFIES CONTROL MODULE OF ANNOUNCEMENT** block 214, the speech module 66 notifies the control module 62 that the announcement has been made to the user 24. At this point at **DISCONNECT TELEPHONE CONNECTION WITH USER** block 215, the control module 62 instructs the line module 64 to terminate the telephone connection and the telephone connection between the security computer 40 and user 24 is severed. At **CONTROL MODULE SENDS AUTHENTICATION MESSAGE TO SERVER PROTOCOL MODULE** block 216, the message that user 24 is authenticated is relayed by control module 62 to server protocol module 116 which is requested to communicate the same to the client protocol module 114. At **SERVER PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO CLIENT PROTOCOL MODULE** block 217, the message is relayed to the client protocol module 114 and thence via a proprietary protocol, at **CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER** block 218, to the host computer 34. The host computer or web server 34 at **HOST COMPUTER GRANTS ACCESS TO USER** block 219 grants access to the authenticated user 24.

In Figure 10 a schematic diagram of the second embodiment of the present invention is shown. For ease of comprehension, where similar components are used, reference designators "200" units higher are employed. In contrast to Figure 1 which describes the out-of-band security networks for computer networks of this invention as applied to the internet or wide area networks, this embodiment describes the application to local area networks. The second embodiment is referred to generally by the reference designator 220. Here the accessor is the computer equipment 222, including the central processing unit and the operating system thereof, and the person or user 224 whose voice is transmittable by the telephone 226 over telephone lines 228. While in this example the biometric parameter monitored is voice patterns as interpreted by voice recognition systems, any of a number of other parameters may be used to identify the person seeking access. The access network 230 is constructed in such a manner that, when user 224 requests access to a high security database 232 located at a host computer 234 through computer 222, the request-for-access is diverted by a router 236 internal to the corporate network 238 to an out-of-band security network 240. Here the emphasis is upon right-to-know classifications within an organization rather than on avoiding entry by hackers. Thus, as the accessor is already within the system, the first level of verification of login identification and password at the host computer is the least significant and the authentication of the person seeking access is the most significant. Authentication occurs in the out-of-band security network 240, which is analogous to the one described in detail above, except the subscriber database becomes layered by virtue of the classification. This is in contradistinction to present authentication processes as the out-of-band security network 240 is isolated from the corporate network 238 and does not depend thereon for validating data. The overview shows the biometric validation which, in this case, takes the form of a voice network 242.

Because many varying and different embodiments may be made within the scope of the inventive concept herein taught, and because many modifications may be made in the embodiments herein detailed in accordance with the descriptive requirement of the law, it is to be understood that the details herein are to be interpreted as illustrative and not in a limiting sense.

WHAT IS CLAIMED IS:

1. An out-of-band security system for granting and denying access to a host computer, said access in response to a demand from an accessor for access to the host computer, said accessor having an associated telephonic device for providing communications to the security system, a login identification accompanying said demand from an accessor for access to the host computer, interception means for receiving and verifying said login identification and transferring authentication of the accessor to said out-of-band security system, said out-of-band security system comprising:

a security computer adapted to receive said demand for access together with said login identification and to communicate with said host computer and with said associated telephonic device of said accessor;

a callback device operable in response to instructions from said security computer to call the accessor;

a subscriber database addressable by the security computer for retrieval of telephone numbers corresponding to said login identification;

said security computer adapted to provide callback instructions to said callback device to connect said associated telephonic device of said accessor to said security computer;

prompt means for instructing said accessor to re-enter predetermined data at and retransmit predetermined data from said associated telephonic device to said out-of-band security system;

comparator means in said security computer for authenticating access demands in response to retransmission of predetermined data from said associated telephonic device of said accessor; and,

said security computer, upon verifying a match between said predetermined data and the re-entered and retransmitted data, providing authentication of the accessor and instructing the host computer to grant access thereto.

2. An out-of-band security system as described in **Claim 1** wherein: said callback device is a telephone; said associated telephonic device of said accessor is a tone generating instrument with a keypad for entering data; and, said prompt means is an auditory message describing data to be entered.

3. An out-of-band security system as described in **Claim 2** wherein said security computer further comprises:

an announcement database therewithin; and

a voice module capable of selecting a prerecorded auditory message from said announcement database and, for prompting the entry of data by said accessor, playing said prerecorded auditory message over said telephone.

4. An out-of-band security system as described in **Claim 3** wherein, upon attaining an access-granted condition said security computer communicates the status to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone.

5. An out-of-band security system as described in **Claim 2** wherein said security computer further comprises:

a voice module, in response to instructions from said security computer, capable of synthesizing an auditory message, and, for prompting the entry of data by said accessor, playing a synthesized auditory message over said telephone.

6. An out-of-band security system as described in **Claim 5** wherein said out-of-band security system further comprises:

an announcement database therewithin and, upon attaining an access-granted condition, said security computer communicates the status to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone.

7. An out-of-band security system as described in **Claim 1** wherein said out-of-band security system further comprises:

a voice recognition program operating in response to instructions from said security computer to authenticate the accessor;

a speech database addressable by the security computer for retrieval of a speech sample of an accessor corresponding to the login identification of said accessor, said computer adapted to provide instructions to connect and disconnect said security computer to and from said associated telephonic device of said accessor;

voice sampling means for instructing said accessor to repeat back and transmit a predetermined auditory statement over said associated telephonic device to said security computer;

voice recognition means in said security computer for authenticating access demands in response to transmission of said predetermined auditory statement received over said associated telephonic device of said accessor; and,

said security computer, upon authenticating a match between the predetermined auditory statement and the transmitted voice data, providing authentication of the accessor and instructing the host computer to grant access.

8. An out-of-band security system for granting and denying access to a web server, said access in response to a demand for access to said web server from an accessor, said accessor having an associated telephonic device for providing communications to said out-of-band security system, said demand presenting an identification number and password of said accessor, said security system comprising:

interception means for receiving and verifying said identification number and password;

a security computer receiving from said interception means said verification of said accessor together with said identification number thereof, said security computer structured to communicate with said web server and with said telephonic device associated with said accessor, said computer adapted to provide instructions to connect and disconnect said security computer to and from said associated telephonic device of said accessor;

an authentication program means, operating out-of-band of said web server, for authenticating an individual demanding access to said web server;

a biometric analyzer operating in response to instructions from said authentication program means to analyze a monitored parameter of said individual;

a biometric parameter database addressable by the biometric analyzer for retrieval of a previously registered sample of said individual, said sample corresponding to the identification number of said accessor;

sampling means for instructing said accessor to provide and transmit a predetermined entry of said monitored parameter over said associated telephonic device to said biometric analyzer;

comparator means in response to a matching analysis between the characteristics of said sample and of said transmission of said predetermined entry of said individual for providing authentication to said security computer; and,

said security computer, upon authenticating a match between the predetermined entry and the sample, providing authentication of the accessor and instructing the web server to grant access.

9. An out-of-band security system as described in **Claim 8** wherein said authentication program is a voice recognition program, said biometric analyzer is a speech pattern analyzer, and said monitored parameter is a speech pattern of said individual.

10. An out-of-band security system as described in **Claim 9** wherein said security computer further comprises:

an announcement database therewithin; and

a voice module capable of selecting a prerecorded auditory message from said announcement database and, for prompting the entry of a predetermined voiced statement by said individual, playing said prerecorded auditory message over said associated telephonic device.

11. An out-of-band security system as described in **Claim 10** wherein, upon attaining an access-granted condition said security computer communicates the status to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said associated telephonic device.

12. An out-of-band security system as described in **Claim 11** further comprising a voice sampling means for instructing said individual to repeat back and transmit a predetermined auditory statement over said associated telephonic device to said security computer.

ABSTRACT OF THE DISCLOSURE

An out-of-band security system is disclosed, which system is for granting and denying access to a host computer in response to a demand from an access-seeking person and computer. The access-seeker has an associated telephonic device for providing communications to the out-of-band security system, and, upon demand, initially presents an identification number and password to the security system. This data is intercepted and transmitted to the security computer. The security computer then communicates with the access-seeker using the associated telephonic device. A biometric analyzer, such as a voice recognition device, operates in response to instructions from the authentication program to analyze a monitored parameter of the individual. The system includes a biometric parameter database addressable by the biometric analyzer for retrieval of previously registered entry of the individual, which entry corresponds to the identification number. A new sample is obtained from the individual and is transmitted to the biometric analyzer over the associated telephonic device. Then a comparator in response to a matching analysis between the characteristics of the sample and those of the predetermined entry provides authentication which the security computer, in turn, communicates to the access-seeker and thereupon instructs the host computer to grant access.

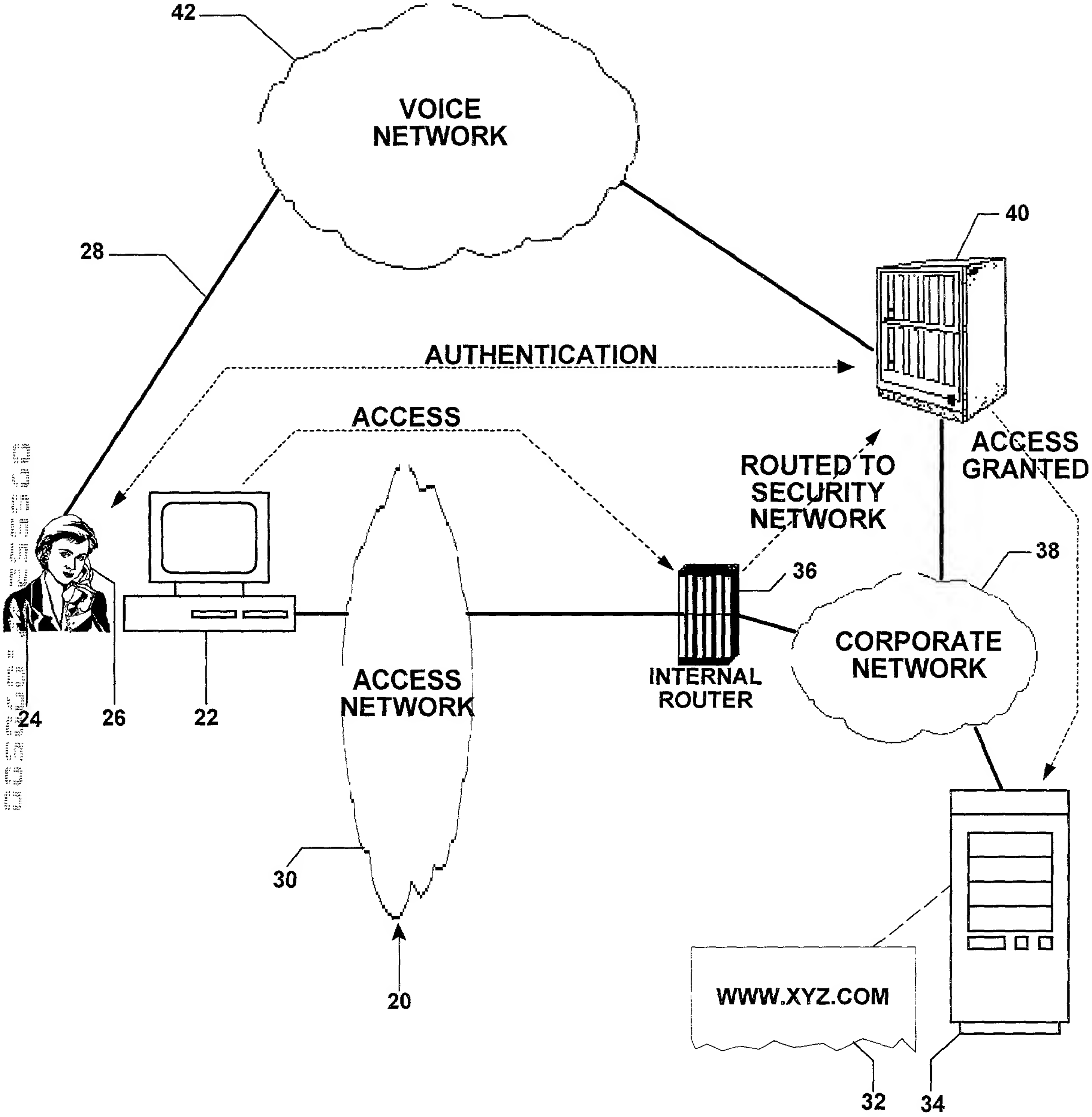
42
VOICE
NETWORK
28
40
AUTHENTICATION
ACCESS
ACCESS
GRANTED
ROUTED TO
SECURITY
NETWORK
38
36
INTERNAL
ROUTER
CORPORATE
NETWORK
ACCESS
NETWORK
24
26
22
30
20
WWW.XYZ.COM
32
34

FIGURE 1

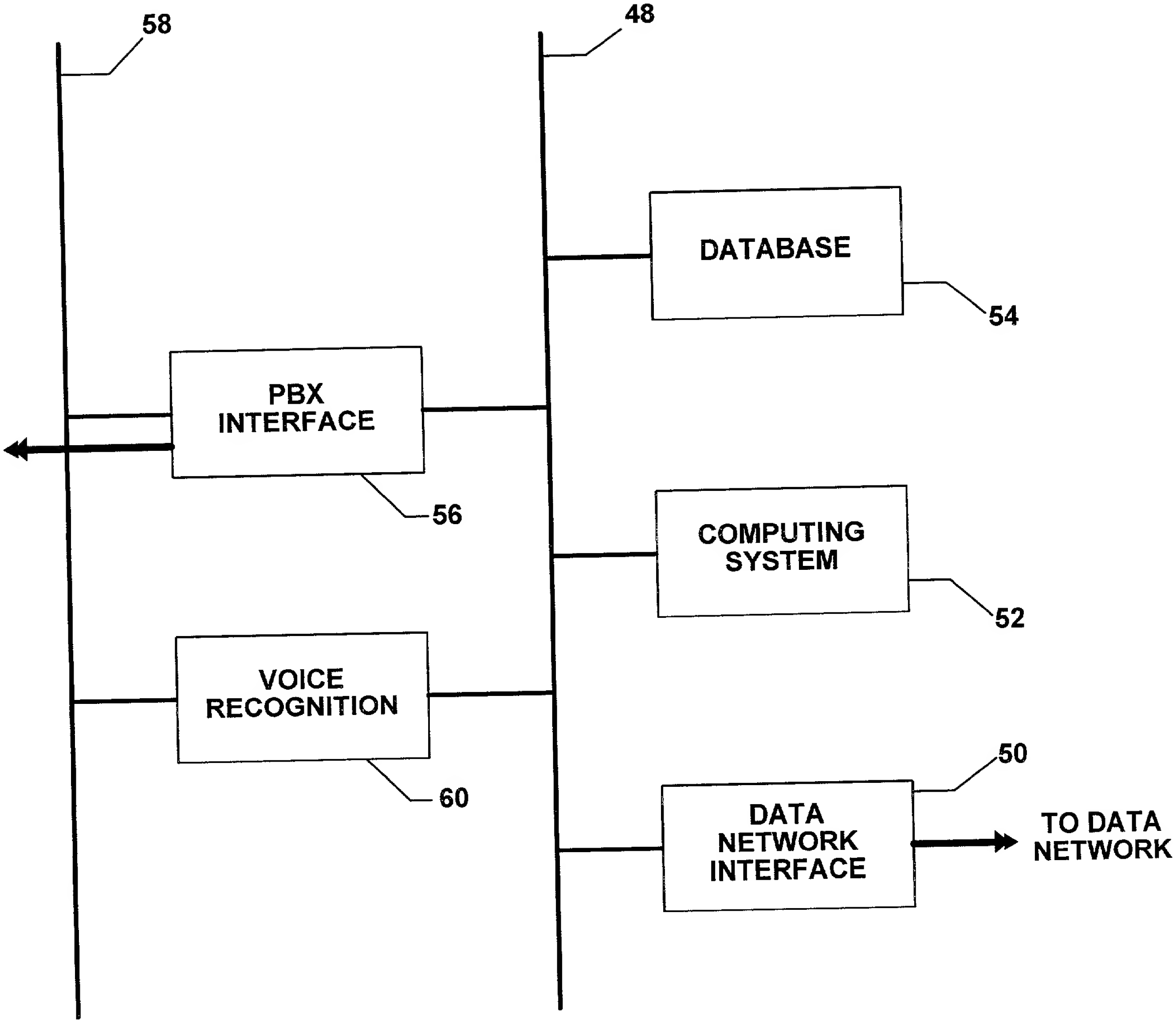
58
48
DATABASE
54
PBX INTERFACE
TO PBX
56
COMPUTING SYSTEM
52
VOICE RECOGNITION
60
50
DATA NETWORK INTERFACE
TO DATA NETWORK

FIGURE 2

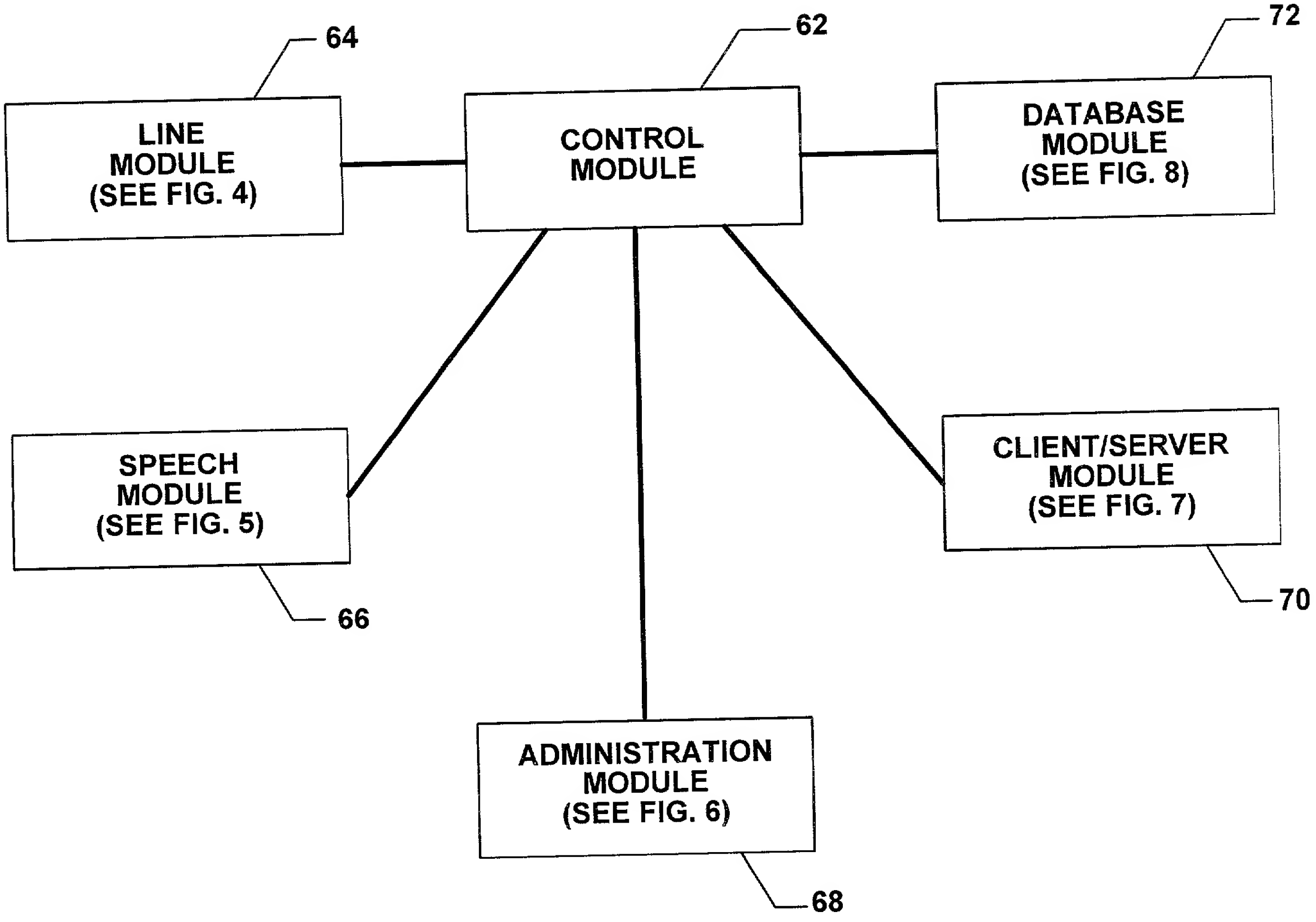
64
62
72
LINE MODULE (SEE FIG. 4)
CONTROL MODULE
DATABASE MODULE (SEE FIG. 8)
SPEECH MODULE (SEE FIG. 5)
CLIENT/SERVER MODULE (SEE FIG. 7)
66
70
ADMINISTRATION MODULE (SEE FIG. 6)
68

FIGURE 3

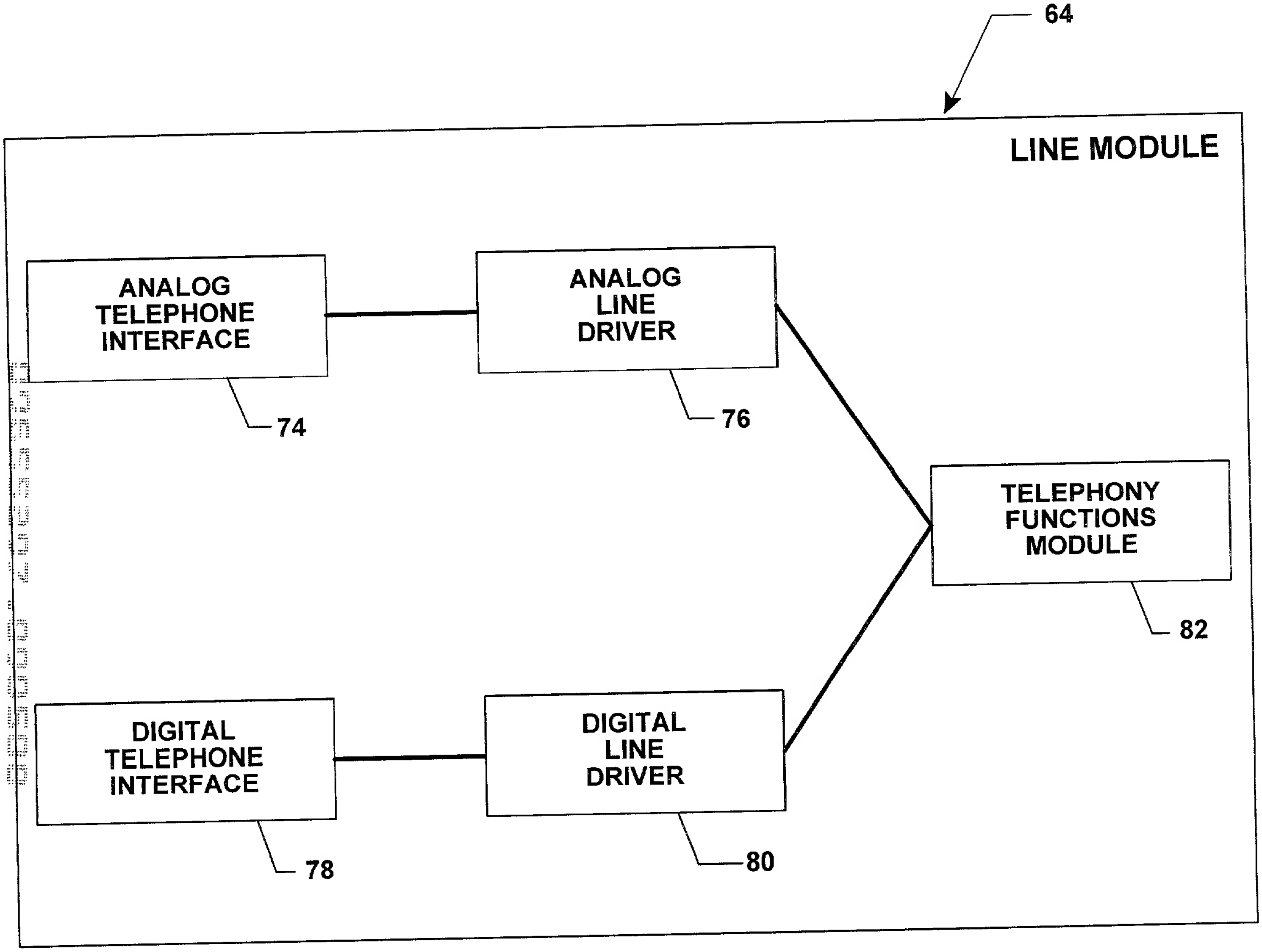
64
LINE MODULE
ANALOG TELEPHONE INTERFACE
74
ANALOG LINE DRIVER
76
TELEPHONY FUNCTIONS MODULE
82
DIGITAL TELEPHONE INTERFACE
78
DIGITAL LINE DRIVER
80

FIGURE 4

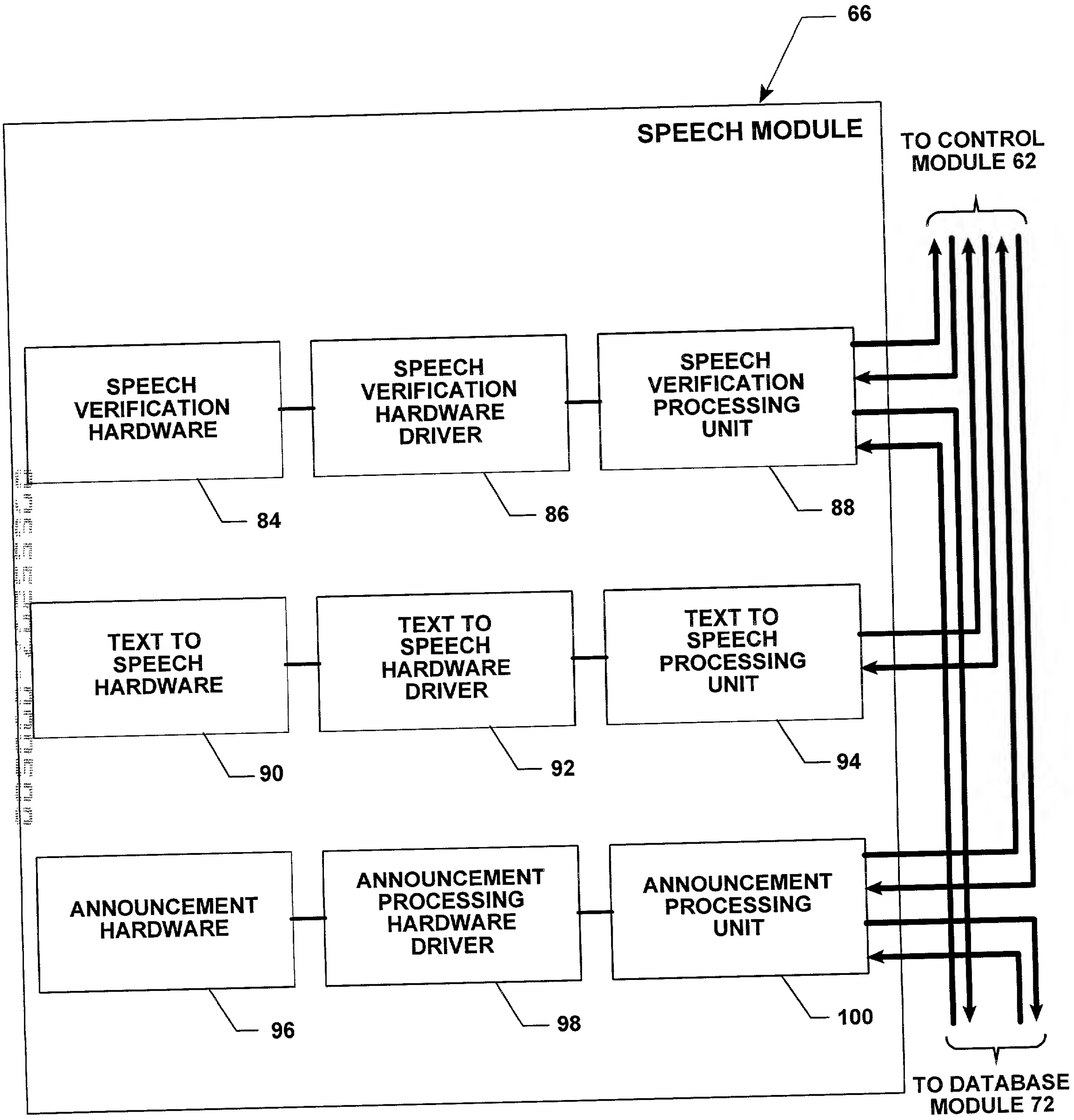
66
SPEECH MODULE
TO CONTROL MODULE 62
SPEECH VERIFICATION HARDWARE
SPEECH VERIFICATION HARDWARE DRIVER
SPEECH VERIFICATION PROCESSING UNIT
84
86
88
TEXT TO SPEECH HARDWARE
TEXT TO SPEECH HARDWARE DRIVER
TEXT TO SPEECH PROCESSING UNIT
90
92
94
ANNOUNCEMENT HARDWARE
ANNOUNCEMENT PROCESSING HARDWARE DRIVER
ANNOUNCEMENT PROCESSING UNIT
96
98
100
TO DATABASE MODULE 72

FIGURE 5

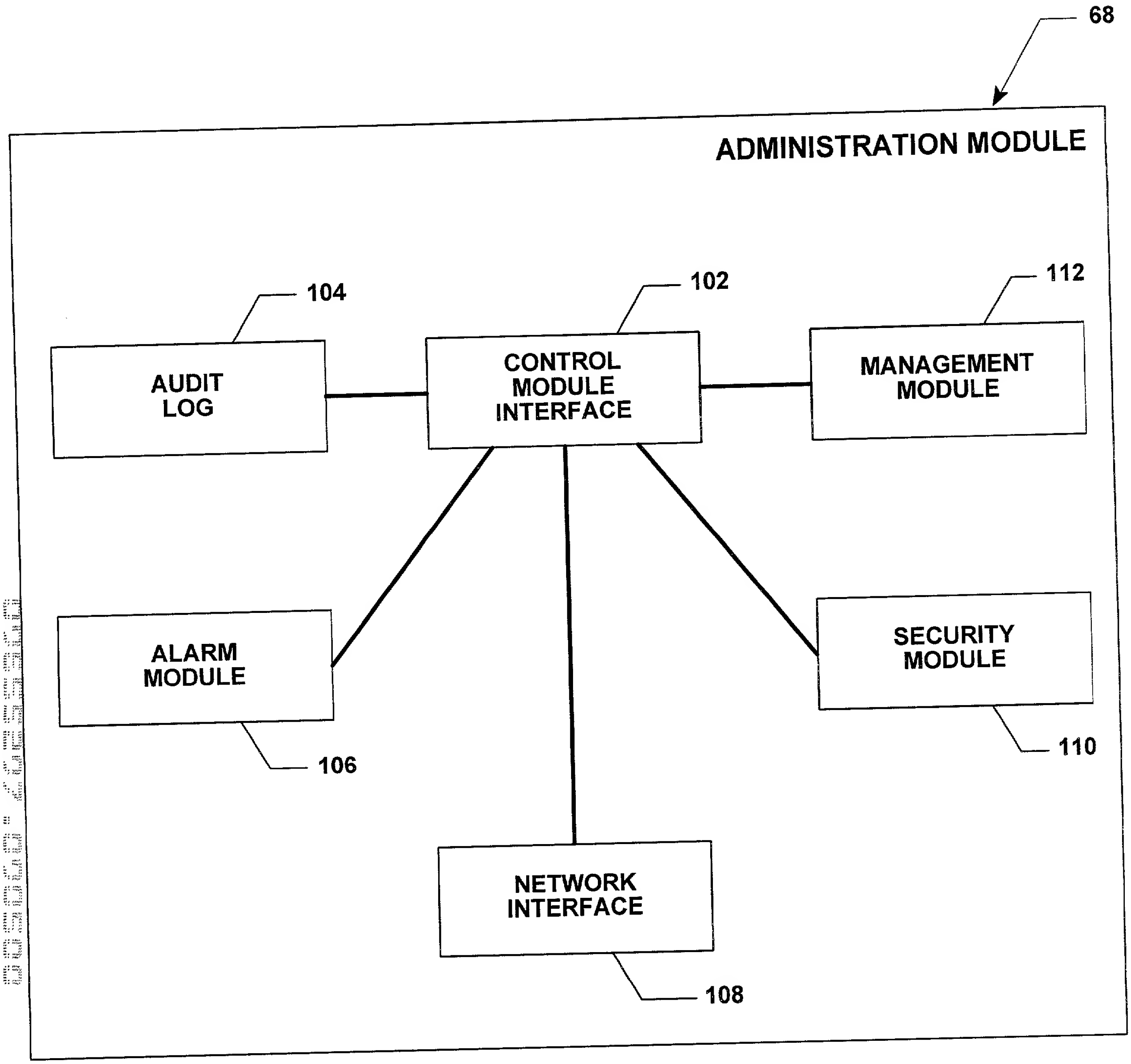
68
ADMINISTRATION MODULE
104
AUDIT LOG
102
CONTROL MODULE INTERFACE
112
MANAGEMENT MODULE
ALARM MODULE
106
SECURITY MODULE
110
NETWORK INTERFACE
108

FIGURE 6

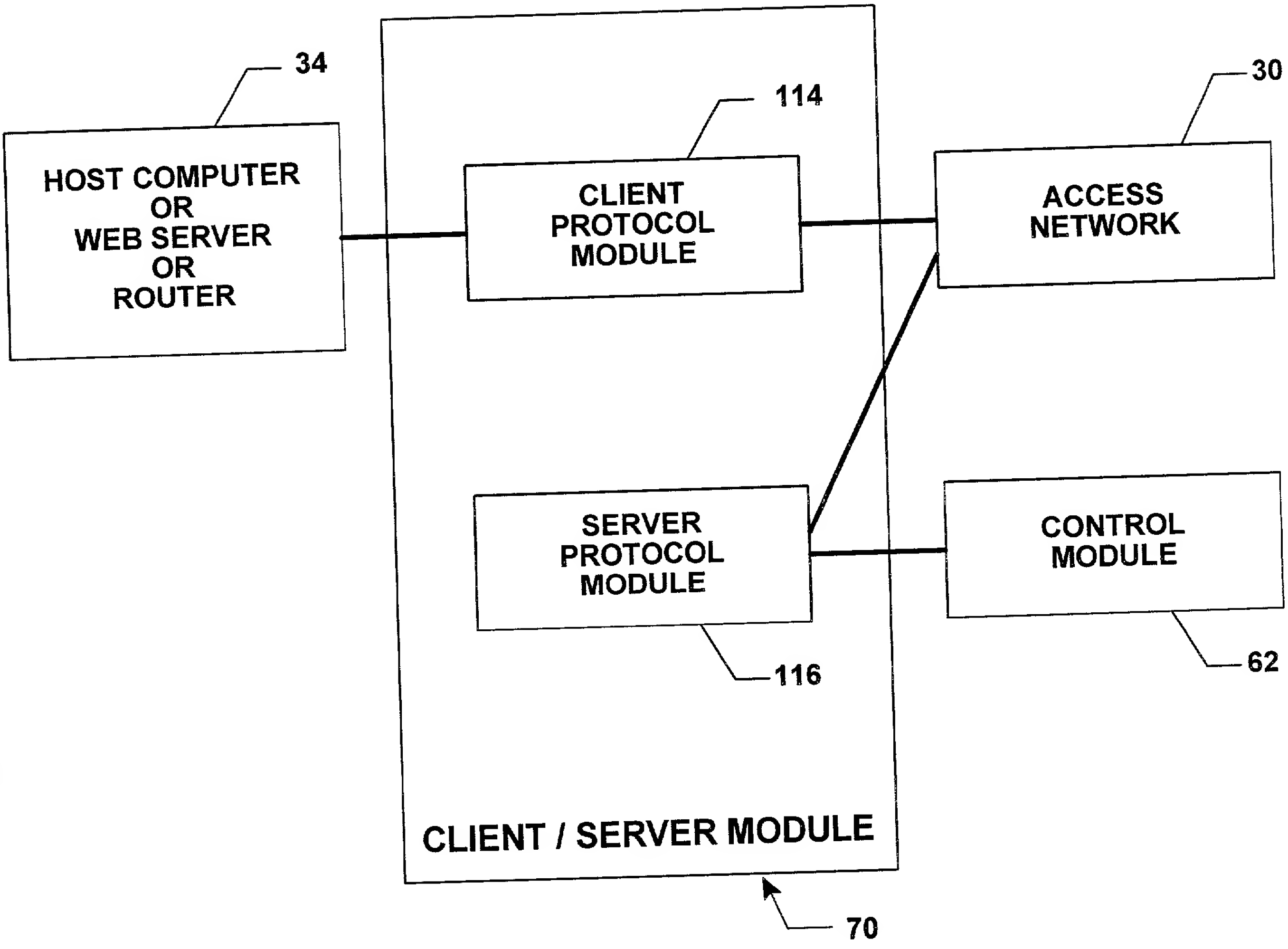
34
HOST COMPUTER OR WEB SERVER OR ROUTER
114
CLIENT PROTOCOL MODULE
30
ACCESS NETWORK
SERVER PROTOCOL MODULE
116
CONTROL MODULE
62
CLIENT / SERVER MODULE
70

FIGURE 7

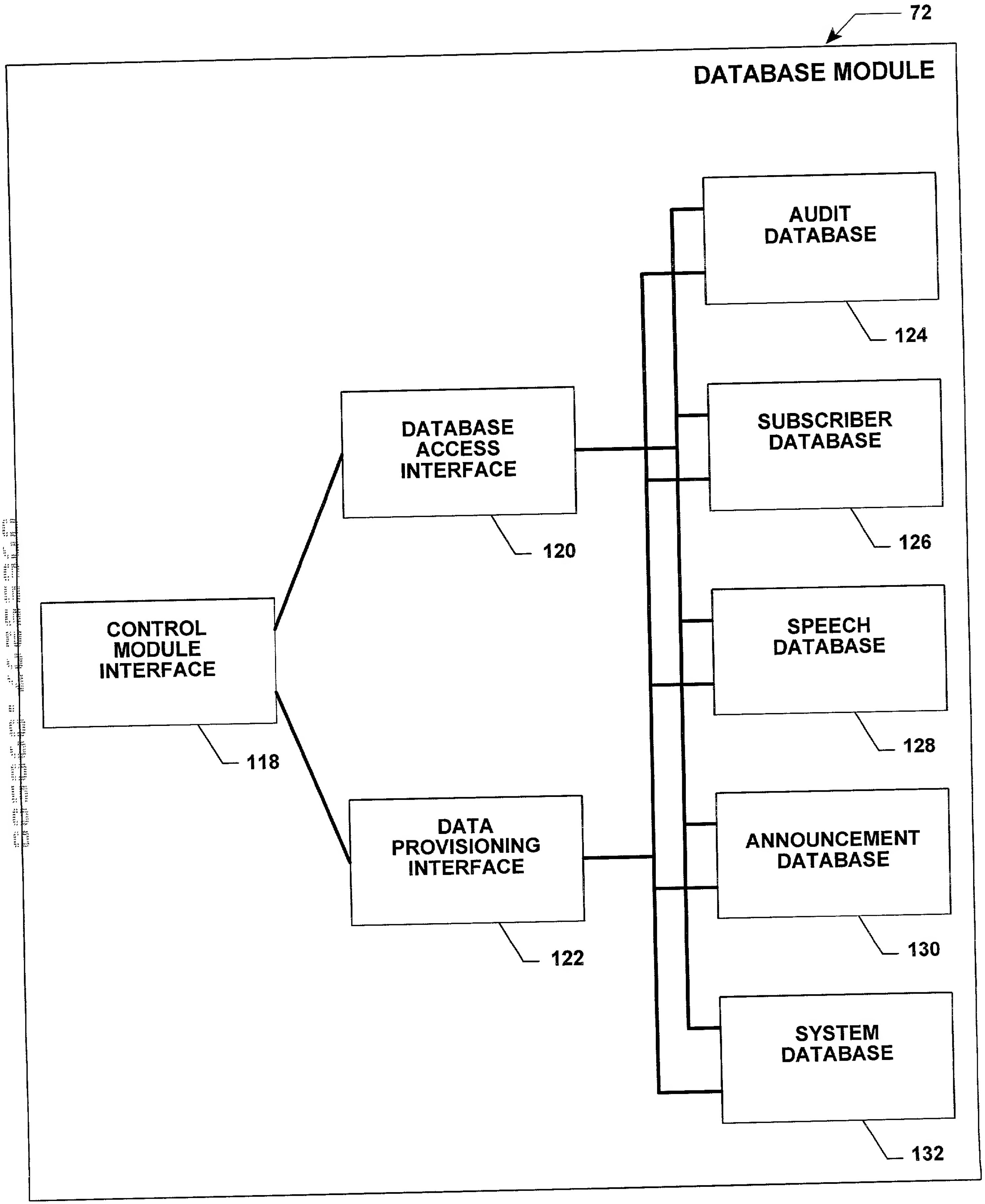
72
DATABASE MODULE
CONTROL MODULE INTERFACE
118
DATABASE ACCESS INTERFACE
120
DATA PROVISIONING INTERFACE
122
AUDIT DATABASE
124
SUBSCRIBER DATABASE
126
SPEECH DATABASE
128
ANNOUNCEMENT DATABASE
130
SYSTEM DATABASE
132

FIGURE 8

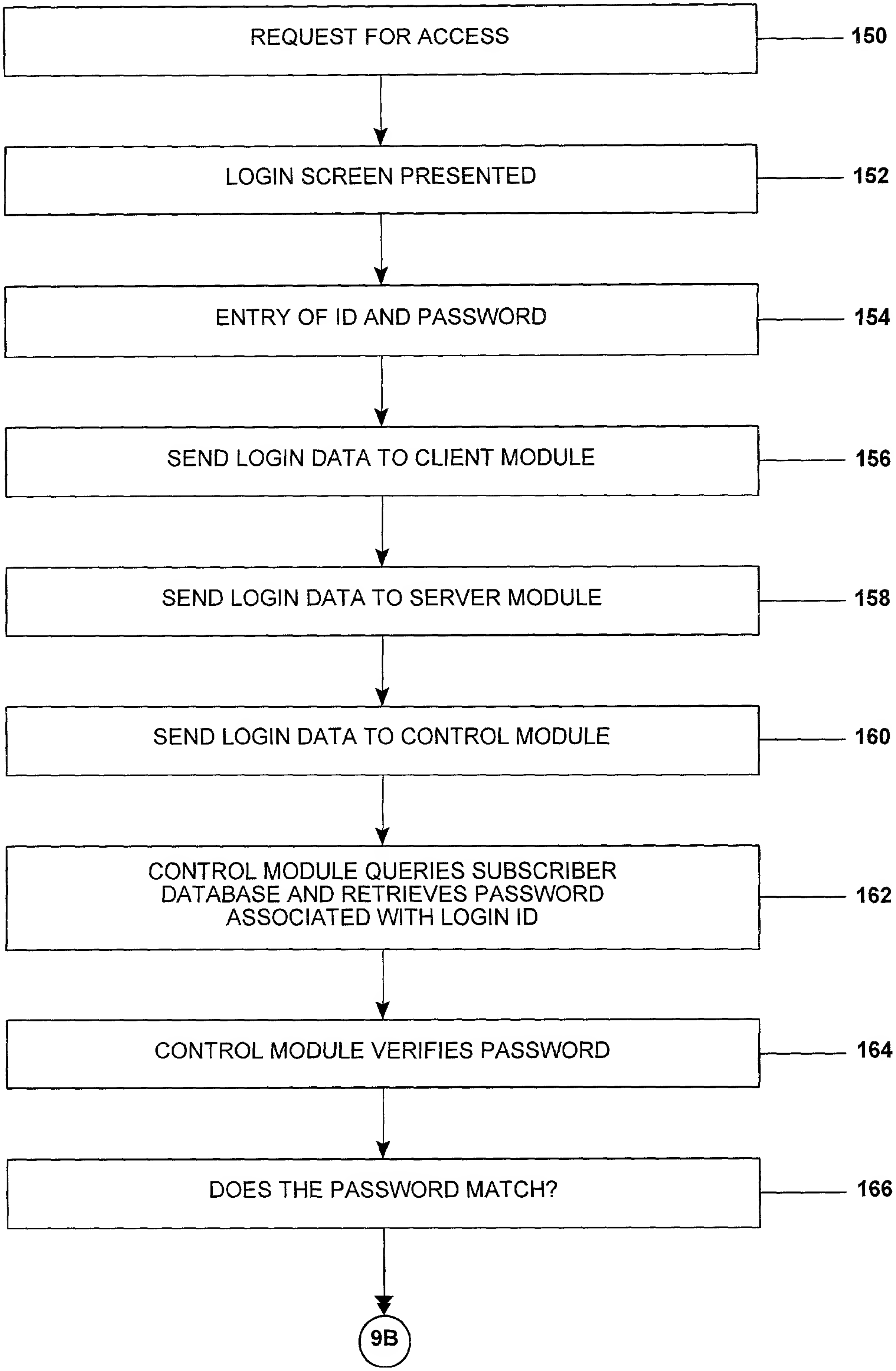
REQUEST FOR ACCESS
150
LOGIN SCREEN PRESENTED
152
ENTRY OF ID AND PASSWORD
154
SEND LOGIN DATA TO CLIENT MODULE
156
SEND LOGIN DATA TO SERVER MODULE
158
SEND LOGIN DATA TO CONTROL MODULE
160
CONTROL MODULE QUERIES SUBSCRIBER DATABASE AND RETRIEVES PASSWORD ASSOCIATED WITH LOGIN ID
162
CONTROL MODULE VERIFIES PASSWORD
164
DOES THE PASSWORD MATCH?
166
9B

FIGURE 9A

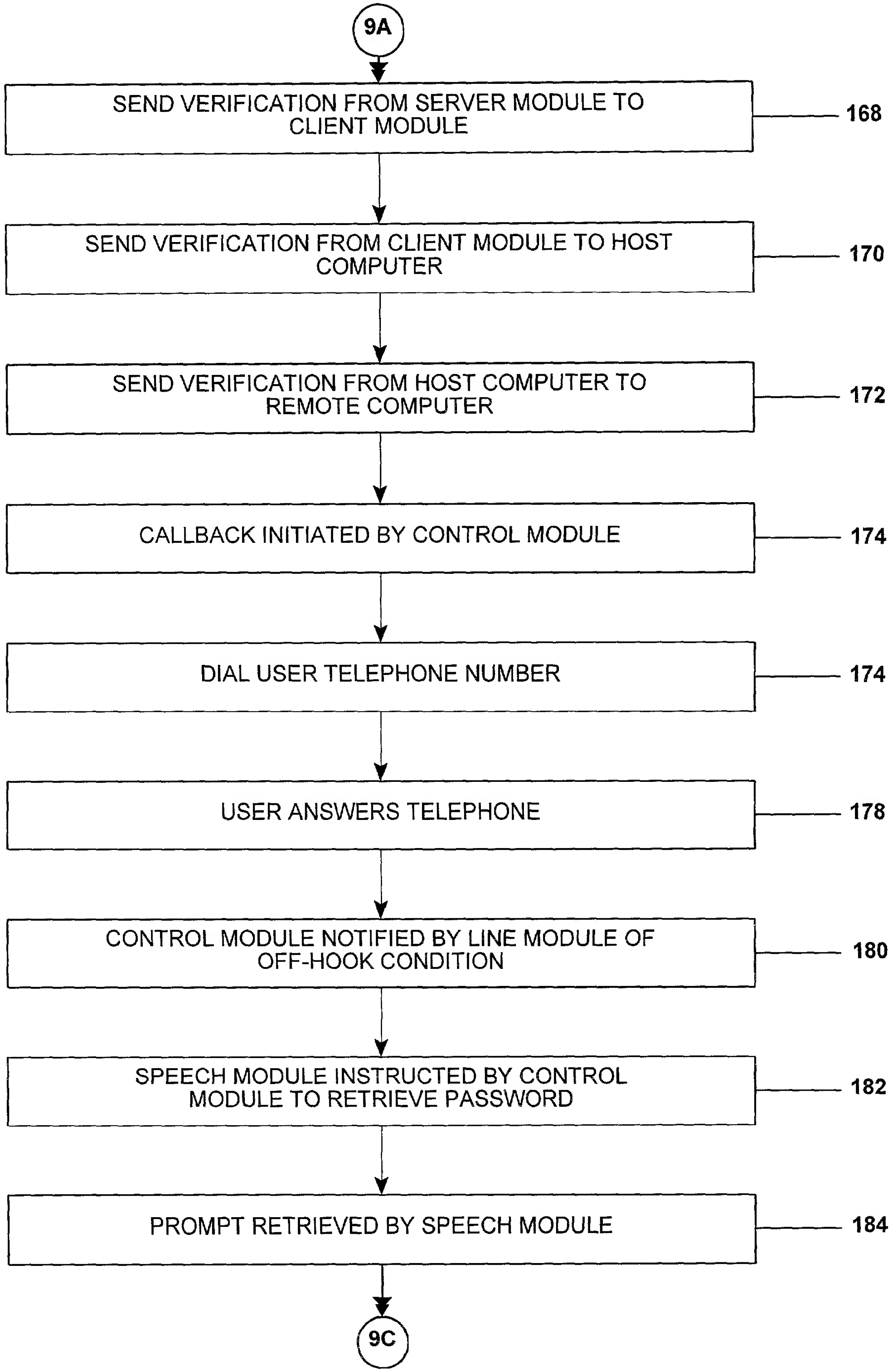
9A
SEND VERIFICATION FROM SERVER MODULE TO CLIENT MODULE
168
SEND VERIFICATION FROM CLIENT MODULE TO HOST COMPUTER
170
SEND VERIFICATION FROM HOST COMPUTER TO REMOTE COMPUTER
172
CALLBACK INITIATED BY CONTROL MODULE
174
DIAL USER TELEPHONE NUMBER
174
USER ANSWERS TELEPHONE
178
CONTROL MODULE NOTIFIED BY LINE MODULE OF OFF-HOOK CONDITION
180
SPEECH MODULE INSTRUCTED BY CONTROL MODULE TO RETRIEVE PASSWORD
182
PROMPT RETRIEVED BY SPEECH MODULE
184
9C

FIGURE 9B

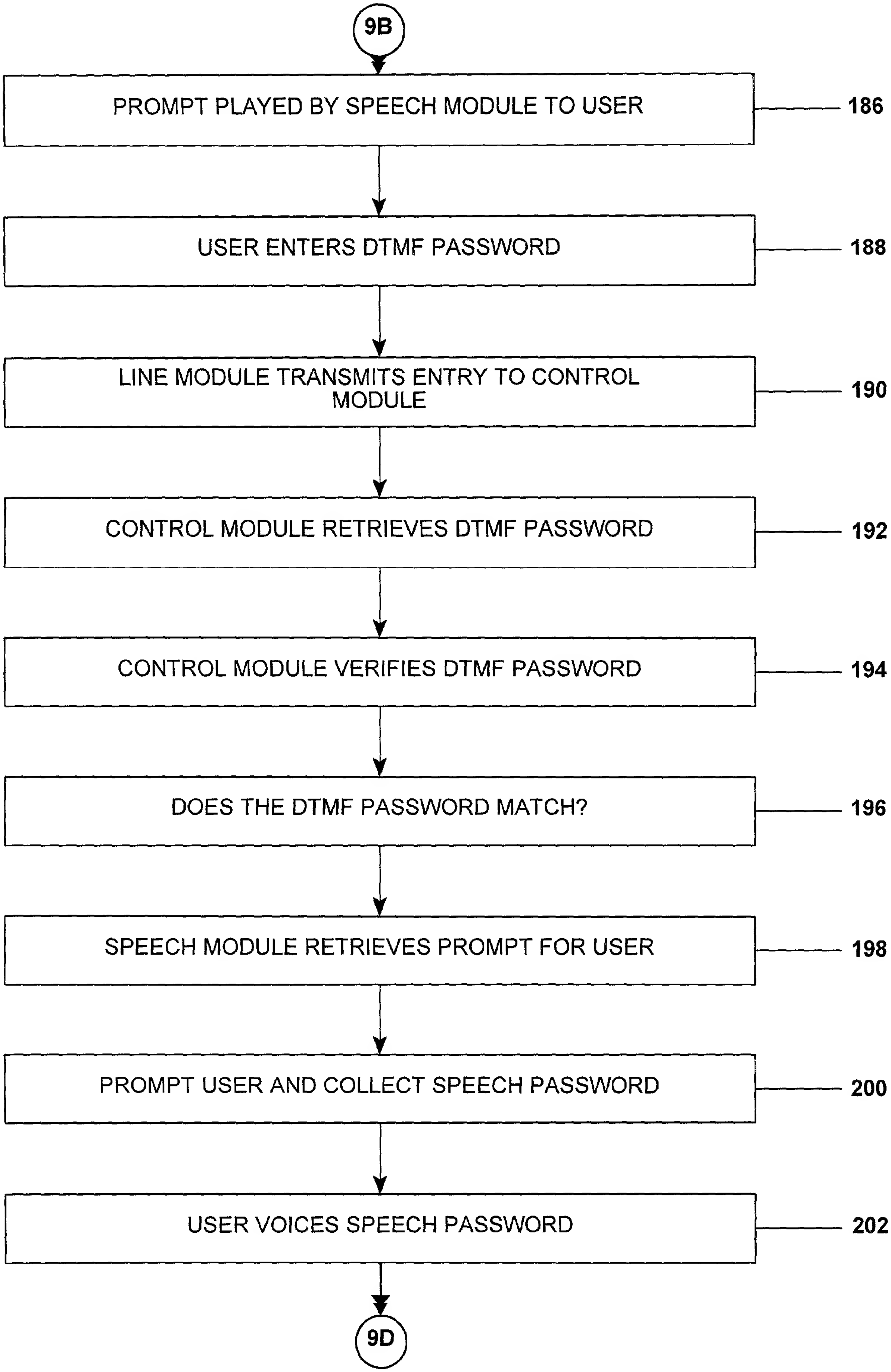
9B
PROMPT PLAYED BY SPEECH MODULE TO USER
186
USER ENTERS DTMF PASSWORD
188
LINE MODULE TRANSMITS ENTRY TO CONTROL MODULE
190
CONTROL MODULE RETRIEVES DTMF PASSWORD
192
CONTROL MODULE VERIFIES DTMF PASSWORD
194
DOES THE DTMF PASSWORD MATCH?
196
SPEECH MODULE RETRIEVES PROMPT FOR USER
198
PROMPT USER AND COLLECT SPEECH PASSWORD
200
USER VOICES SPEECH PASSWORD
202
9D

FIGURE 9C

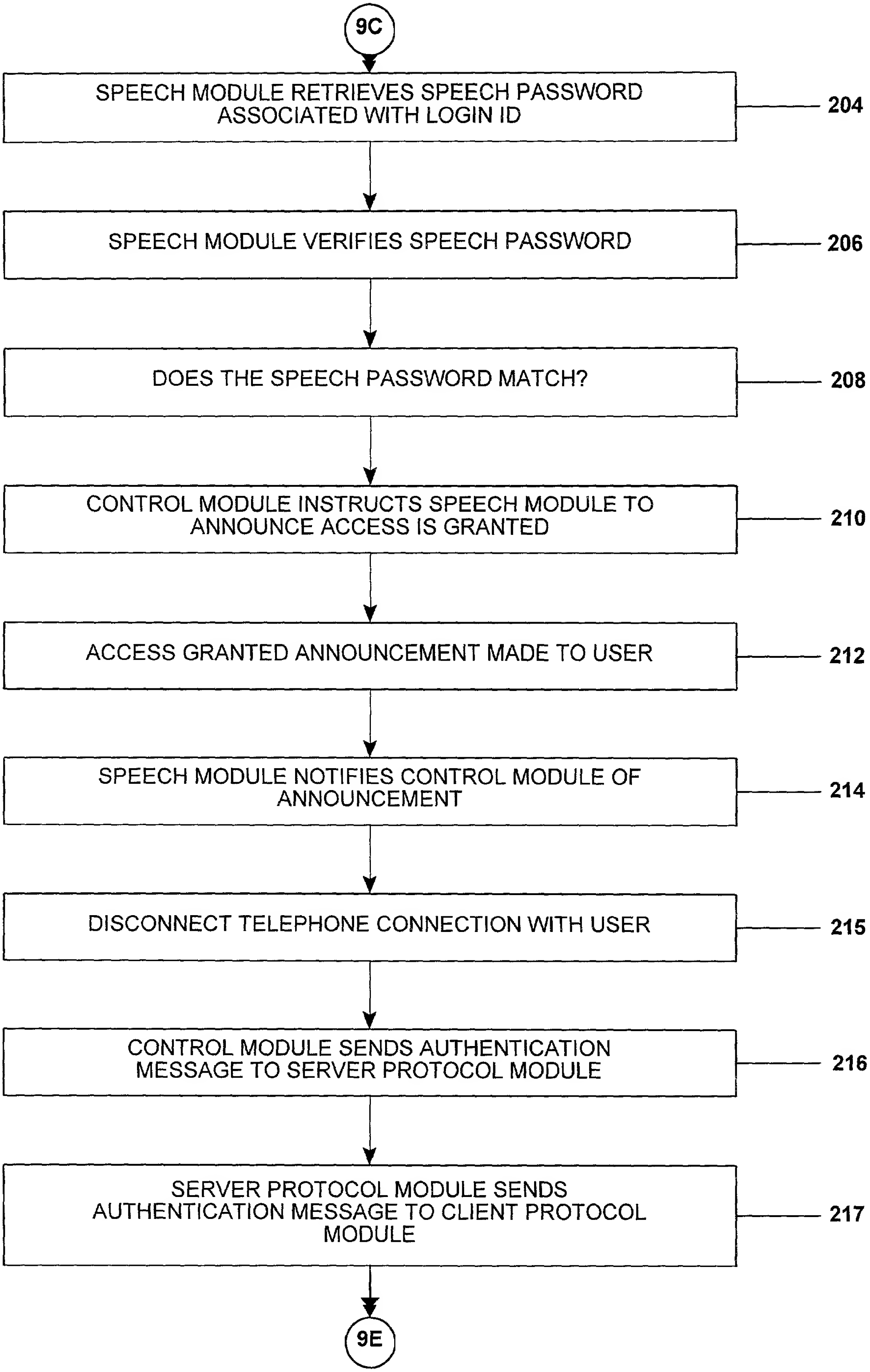
9C
SPEECH MODULE RETRIEVES SPEECH PASSWORD ASSOCIATED WITH LOGIN ID
204
SPEECH MODULE VERIFIES SPEECH PASSWORD
206
DOES THE SPEECH PASSWORD MATCH?
208
CONTROL MODULE INSTRUCTS SPEECH MODULE TO ANNOUNCE ACCESS IS GRANTED
210
ACCESS GRANTED ANNOUNCEMENT MADE TO USER
212
SPEECH MODULE NOTIFIES CONTROL MODULE OF ANNOUNCEMENT
214
DISCONNECT TELEPHONE CONNECTION WITH USER
215
CONTROL MODULE SENDS AUTHENTICATION MESSAGE TO SERVER PROTOCOL MODULE
216
SERVER PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO CLIENT PROTOCOL MODULE
217
9E

FIGURE 9D

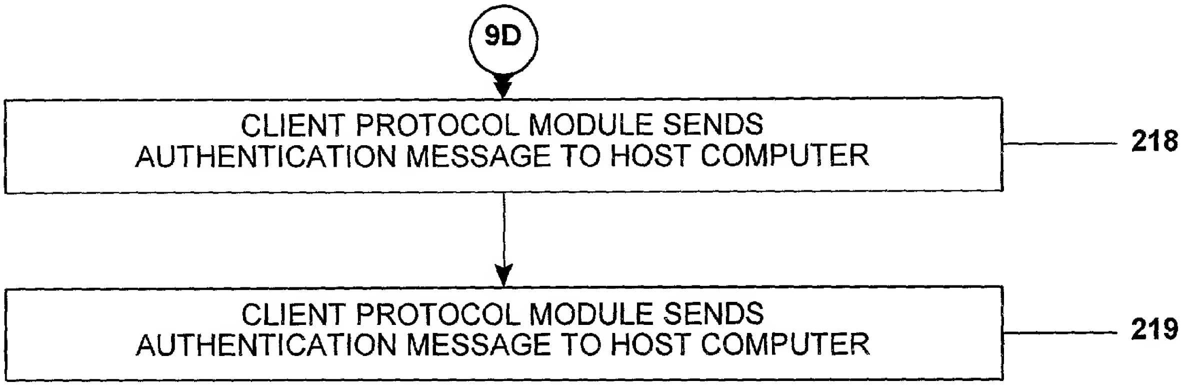
9D
CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER
218
CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER
219

FIGURE 9E

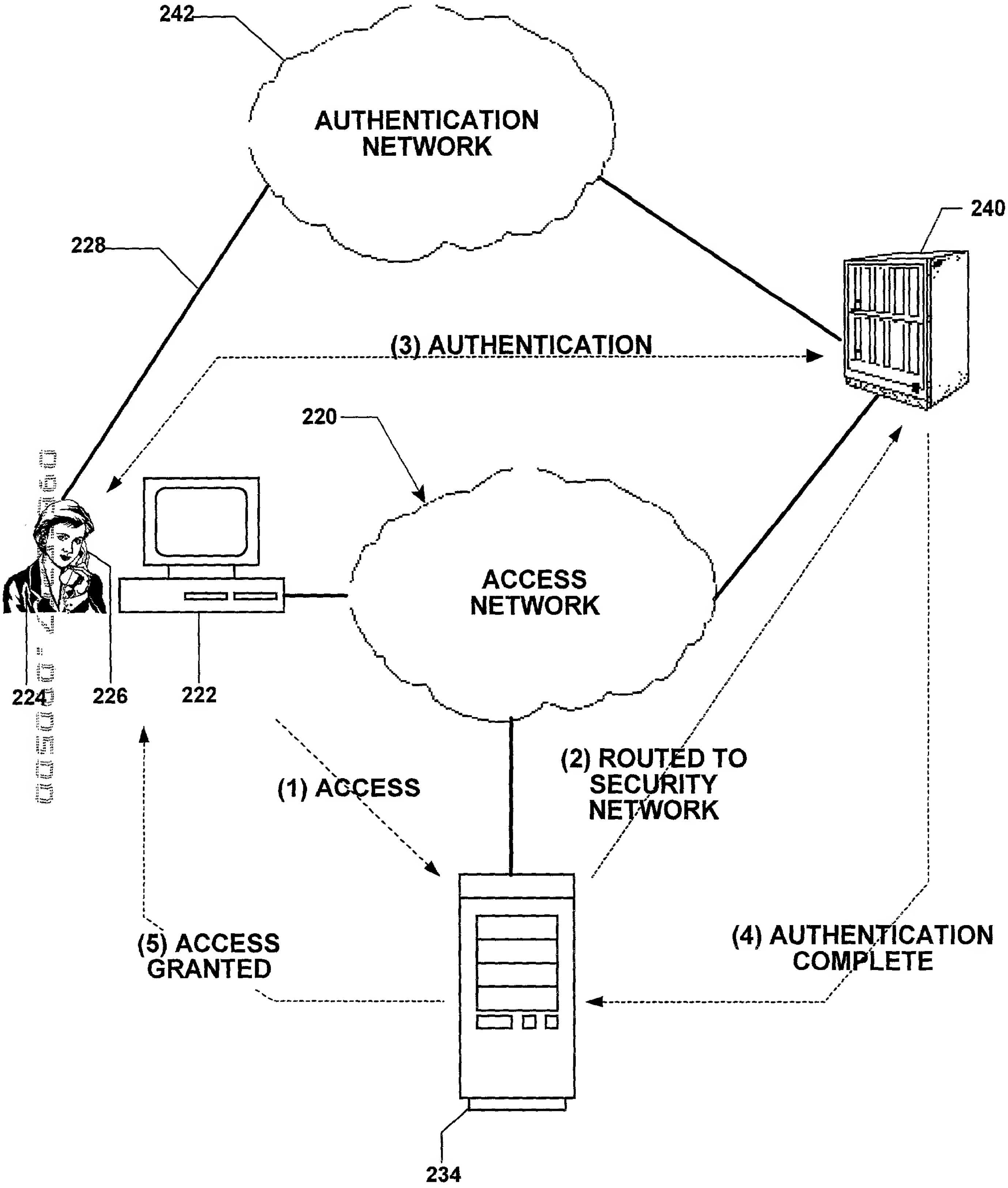
242
AUTHENTICATION NETWORK
240
228
(3) AUTHENTICATION
220
ACCESS NETWORK
224
226
222
(1) ACCESS
(2) ROUTED TO SECURITY NETWORK
(5) ACCESS GRANTED
(4) AUTHENTICATION COMPLETE
234

FIGURE 10

Attorney's Docket N0 PNE- 203
PATENT

COMBINED DECLARATION AND POWER OF ATTORNEY

(Original, Design,Supplemental)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type:

☒ **original**
□ **design**
□ **supplemental**

INVENTORSHIP IDENTIFICATION

Warning: If the inventors are each not the inventors of all the claims, an explanation of the facts, including the ownership of all the claims at the time the last claimed invention was made, should be submitted.

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and sole inventor (*if only one name is listed below*) original, first and joint inventor *(if plural names are listed below)* of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

OUT-OF-BAND SECURITY NETWORKS FOR COMPUTER APPLICATIONS

SPECIFICATION IDENTIFICATION

The specification is attached hereto.

Note: "The following combinations of information supplied in an oath or declaration filed on the application filing date with a specific are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 CFR 1.63:

"(1) name of inventor(s), and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration on filing;

"(2) name of inventor(s), and attorney docket number which was on the specification as filed; or

"(3) name of inventor(s), and title which was on the specification as filed."

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s).

I acknowledge the duty to disclose information, which is material to patentability as defined in 37 CFR § 1.56 and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent,

POWER OF ATTORNEY

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Siegmar Silber, Esq.	Registration No. 26,233
Lawrence G. Fridman, Esq.	Registration No. 31,615

(check the following item, if applicable)

□Attached, as part of this declaration and power of attorney, is the authorization of the above-named attorney(s) to accept and follow instructions from my representative(s).

SEND CORRESPONDENCE TO

Siegmar Silber, Esq.
SILBER & FRIDMAN
66 Mount Prospect Avenue
Clifton, NJ 07013-1918

DIRECT TELEPHONE CALLS TO:

Siegmar Silber, Esq.
(973) 779-2580
FAX: (973) 779-4473

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Note: Carefully indicate the family (or Last) name, as it should appear on the filing receipt and all other documents.

Full name of sole or first Inventor

RAM		PEMMARAJU
(Given Name)	**(Middle Initial or Name)**	**(Family or Last Name)**

Inventor's signature____________________
Date 09/01/2000 **Country of Citizenship** U. S. A.
Residence 8 PONDEROSA LANE, OLD BRIDGE, NEW JERSEY 08857
Post Office Address Same

Full Name of second joint inventor, if any

(Given Name)	**(Middle Initial or Name)**	**(Family or Last Name)**

Inventor's signature____________________
Date__________ **Country of Citizenship**__________ **Residence**____
____________________ **Post Office Address**___

Full Name of third joint inventor, if any

(Given Name)	**(Middle Initial or Name)**	**Family (or Last Name**

Inventor's signature____________________
Date__________ **Country of Citizenship**__________
Residence____________________
Post Office Address____________________

(Check proper box for any of the following added pages(s) that form a part of this declaration)

* * * *

☐ **Authorization of attorney(s) to accept and follow instructions from representative**

* * * *

* * * *

(If not further pages form a part of this Declaration, then end this Declaration with this page and check the following item)

☒